Nina:

Below are our comments on your alternative approach to risk assessment. We appreciate the thought that went into it (it is an interesting approach), but do have the following comments and recommendations. The recommendations will help us reach the goal of moving more threats to either the "low" or "no further action required" level.

Comments on Revised Methodology

We do not think one should simply assume the motivation level of human threat agents. External agents could very well be lacking in motivation, just as inside privileged users could be very highly motivated. We would definitely not assume that inside privileged threat agents are unmotivated—most attacks occur from within. A background check/screening does not really reduce anyone's motivation, nor does having administrator-level access.

The new proposed methodology mixes "threat realization" with "countermeasure effectiveness." These two should be treated separately. Means, opportunity, and motivation should all still be covered under "realization."

Did the wording in the "threat likelihood" table change? (The column of the left used to be labeled "Realization," and not "Threat Agent."). Not sure that "Threat Agent" is a clear term.

We are confused about the difference between "realization" and "likelihood." Before, "realization" was one of the factors in determining likelihood; now, it seems as if "realization" is the end in itself. Remember: Risk = Impact x *Likelihood.* We think it should be called "threat likelihood," rather than "threat realization," to be consistent with NIST terminology.

It is not true that secure systems with high-impact data do not give outside access to this data—for example, banks can access detailed loan information, as can students.

Recommendations

Leave both the threat likelihood and impact tables the same as they were before.

Another way to reduce the realization ranking to "low" would be to back this up with *quantitative* analysis—eg, "how many times in the past xx years has a system been hacked by a privileged insider"?

With regard to IG findings and associated recommendations, we could argue that if implementing IG recommendations would NOT increase the overall level of existing countermeasure effectiveness (ie, it would not reduce the overall risk level), then those recommendations would not have to be implemented, and the level of risk might be an acceptable level.

Bob Ingwalson, Brian Fuller, Chuck Tobler